What is claimed:

1. A method of improving security processing in a computing network, comprising steps of:

providing security processing in an operating system kernel;

providing an application program which makes use of the operating system kernel during execution;

executing the application program; and

selectably securing at least one communication of the executing application program using the provided security processing in the operating system kernel.

2. The method according to Claim 1, further comprising the step of:

configuring one or more ports used by the provided application program such that communications using the configured ports are to be secured; and

wherein the selectably securing step then secures all communications using the configured ports.

3. The method according to Claim 2, wherein the provided application program does not include code for security processing.

4. The method according to Claim 2, wherein the configuring step further comprises specifying information to be used by the selectably securing step.

5. The method according to Claim 4, wherein the specified information comprises one or

more of: authentication information; cipher suites options; and security key input information.

6. The method according to Claim 2, wherein the configuring step comprises one or more of: providing port definition statements; setting environment variables; and using job control language.

7. The method according to Claim 1, further comprising the step of providing, in the secure processing, support for one or more security directives.

8. The method according to Claim 7, further comprising the step of invoking, during execution of the provided application program, one or more of the provided security directives.

9. The method according to Claim 7, wherein the provided security directives comprise one or more of: access capability for a client certificate; access capability for a client identifier; a request to start operation of the selectably securing step; and a request to stop operation of the selectably securing step.

10. The method according to Claim 8, wherein the provided security directives include an access capability for a client certificate, and wherein the invoking step invokes the access capability, and further comprising the step of returning the client certification from the provided security processing to the executing application program in response to the invocation.

11. The method according to Claim 8, wherein the provided security directives include an access capability for a client identification, and wherein the invoking step invokes the access capability, and further comprising the step of returning the client identification from the provided security processing to the executing application program in response to the invocation.

12. The method according to Claim 1, further comprising the steps of:

providing, in the secure processing, support for a security directive that requests the selectably securing step to begin operating; and

invoking the security directive; and

wherein the selectably securing step then secures all communications of the executing application program.

13. The method according to Claim 1, further comprising the steps of:

providing, in the secure processing, support for a security directive that requests the selectably securing step to stop operating; and

invoking the security directive; and

wherein the selectably securing step then stops securing communications of the executing application program.

14. The method according to Claim 12, wherein the security directive specifies information to be used by the selectably securing step.

15. The method according to Claim 14, wherein the specified information comprises one or more of: authentication information; cipher suites options; and security key input information.

16. The method according to Claim 12, wherein a decision to invoke the security directive is made by the executing application program.

17. The method according to Claim 12, wherein a decision to invoke the security directive is made by carrying out, by the executing application program, a security negotiation protocol.

18. The method according to Claim 1, wherein the provided application program includes calls that invoke security processing, and further comprising steps of:

intercepting, in the provided security processing, the calls; and

executing, responsive to the interception, corresponding security functions.

19. The method according to Claim 1, wherein the provided application program includes calls that invoke security processing, and further comprising step of interpreting, in the provided security processing, the calls as being non-operative.

20. The method according to Claim 18, wherein the provided application program may be executed on a system which does not include the provided security processing in the operating system kernel, in which case the calls operate to perform security processing instead of the selectably securing step.

21. The method according to Claim 1, wherein the provided security processing operates in a Transmission Control Protocol layer of the operating system kernel.

22. The method according to Claim 1, wherein the provided security processing implements Secure Sockets Layer.

23. The method according to Claim 1, wherein the provided security processing implements Transaction Layer Security.

24. A system for improving security processing in a computing network, comprising:

means for performing security processing in an operating system kernel;

means for executing an application program which makes use of the operating system kernel during execution; and

means for selectably securing at least one communication of the executing application program using the means for performing security processing, in a manner which is transparent to the executing application program.

25. A system for improving security processing in a computing network, comprising:

means for performing security processing in an operating system kernel;

means for executing an application program which makes use of the operating system kernel during execution; and

means for selectably securing at least one communication of the executing application program using the security processing performed in the operating system kernel.

26. A computer program product for improving security processing in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for performing security processing in an operating system kernel;

computer-readable program code means for executing an application program which makes use of the operating system kernel during execution; and

computer-readable program code means for selectably securing at least one communication of the executing application program using the security processing performed in the operating system kernel.